

This is a repository copy of *The STRUCTURES Project : Strategies for The impRovement of critical infrastrUCTure Resilience to Electromagnetic attackS.*

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/91328/>

Version: Submitted Version

Proceedings Paper:

Dawson, John F orcid.org/0000-0003-4537-9977 (2013) The STRUCTURES Project : Strategies for The impRovement of critical infrastrUCTure Resilience to Electromagnetic attackS. In: IET Seminar on: Extreme Electromagnetics - The Triple Threat to Infrastructure. .

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.



The STRUCURES Project

**Strategies for The impRovement of critical infrastrUCTUre
Resilience to Electromagnetic attackS**

John F Dawson

University of York

john.dawson@york.ac.uk

IET Extreme Electromagnetics – 14 Jan 2013



Project Overview

- 3 year Framework 7 (EU) funded (Jul 12 – Jun 15)
- 12 partners
 - Industry: IDS, Rheinmetall, Montena, Navigate
 - Universities: York, Hannover, Twente, Hamburg, Turin, Wuppertal, Lausanne, Western Switzerland
- End users including:
 - CIGRE, Swiss Electromagnetics Research & Engineering Centre, Thales, Telecom Italia, and more....



	Industry		
1	I.D.S. - INGEGNERIA DEI SISTEMI - S.P.A.	IDS	Italy
9	RHEINMETALL WAFFE MUNITION GMBH	RWM	Germany

	Universities		
2	ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE	EPFL	Switzerland
3	HAUTE ECOLE SPECIALISEE DE SUISSE OCCIDENTALE	HES-SO	Switzerland
4	UNIVERSITY OF YORK	UoY	United Kingdom
6	HELMUT SCHMIDT UNIVERSITAT UNIVERSITAT DER BUNDESWEHR, HAMBURG	HSU	Germany
7	GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER	LUH	Germany
8	BERGISCHE UNIVERSITAET WUPPERTAL	BUW	Germany
10	UNIVERSITEIT TWENTE	UT	Netherlands
13	POLITECNICO DI TORINO	POLITO	Italy

Implementing Team

	Research centres		
11	ISTITUTO SUPERIORE MARIO BOELLA SULLE TECNOLOGIE DELL'INFORMAZIONE E DELLE TELECOMUNICAZIONI	ISMB	Italy

	SME		
5	MONTENA TECHNOLOGY SA	Montena	Switzerland
12	NAVIGATE CONSORTIUM CONSORZIO	NAVI	Italy

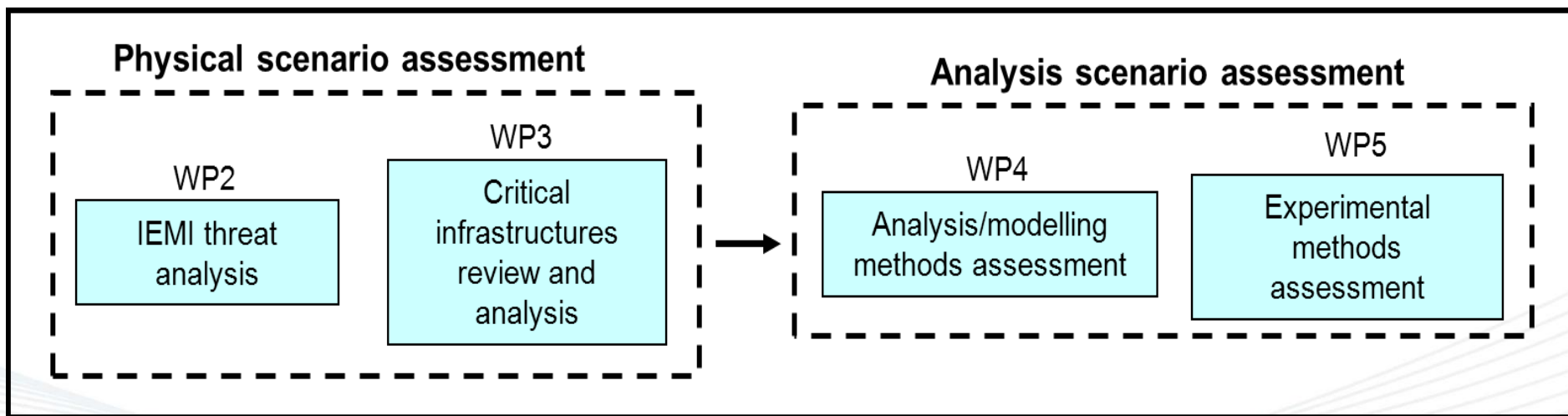


Project Aims

- Bring together existing research in IEMI
- Analysis of risks to critical infrastructure
- Protection and detection
- Guidelines for end users and policy makers
- Interaction with end users during project



Phase 1

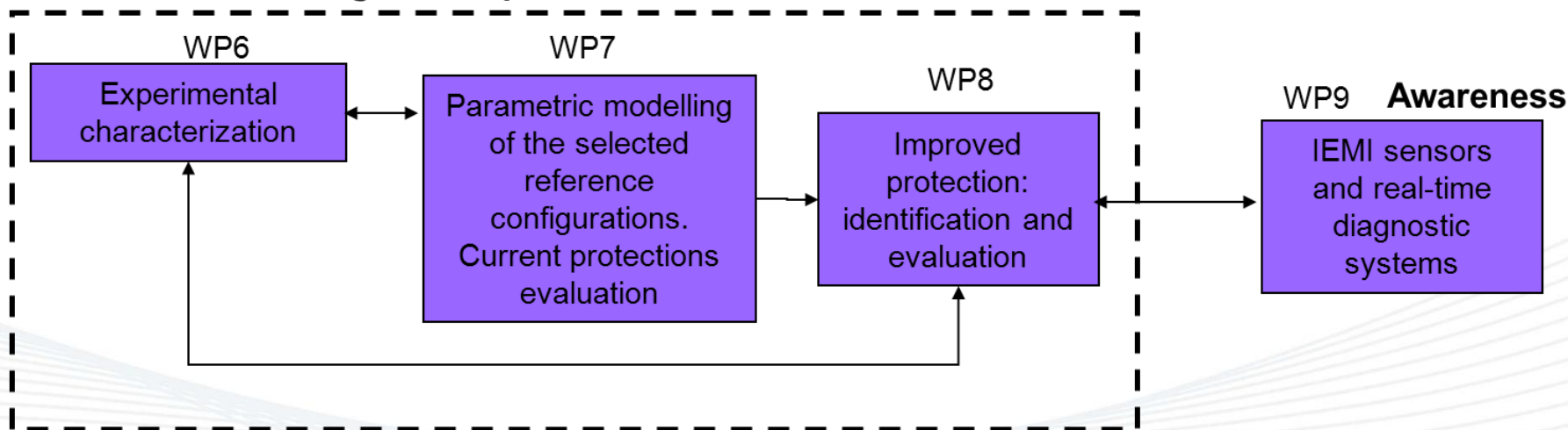


- Assessment of the scenarios of interest, from the physical point of view
- Defining Modelling and measurements issues for Phase 2.



Phase 2

Risk investigation & protection



- Investigation of IEMI effects on the critical infrastructures, sub-systems and functions identified in Phase 1
- Identification of possible cost-effective technologies able to improve the infrastructure resilience.



Phase 3

WP10

Guidelines,
methodologies etc
for IEMI protection

To policy makers...

- Pre-regulatory documentation:
comprising guidelines, methodologies, tools,
recommendations, optimal criteria etc.



End Users

Important for assuring the project is relevant.

What is expected from End Users (at different levels of participation):

- 1. Access to the project outputs (participation to dissemination events once a year – costs will be charged to the project)**
- 2. Support to the project requirement definition (entering the discussion about requirements during the dissemination events and, if needed, answering a questionnaire)**



End Users

3. Support to the characterization of the specific Critical Infrastructures (participation to 1 – 2 half a day meetings with the project staff)

**UK Contact: John Dawson, University of York
john.dawson@york.ac.uk**



Resources

STRUCTURES web site: <http://www.structures-project.eu/>

Hoad, R. & Radasky, W. A. (2012). High Power Electromagnetic Disturbances to the Smart Grid and the Status of Protection Standards. , Available from:
<http://www.theiet.org/communities/electromagnetics/energy-and-power/disturbances-smart-grid.cfm>

Sabath, F. (2012). What can be learned from documented Intentional Electromagnetic Interference (IEMI) attacks?. EUROEM 2012, Available from:
<http://www.ece.unm.edu/summa/notes/AMEREM-EUROEM/EUROEM2012-final-10July2012NPA%20-SUMMA.pdf>

Genender, E.; Mleczo, M.; Döring, O.; Garbe, H. & Potthast, S. (2011). Fault tree analysis for system modeling in case of intentional EMI. Advances in Radio Science, 9 297-302 , Available from: <http://www.adv-radio-sci.net/9/297/2011/>

Hagmann, J. H.; Dickmann, S. & Potthast, S. (2011). Application and propagation of transient pulses on power supply networks. EMC Europe 2011 York, 7-12
<http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6064642>

Abrams, M. (2003). Dawn of the E-bomb. IEEE Spectrum, November 24-30 , Available from:
<http://spectrum.ieee.org/biomedical/devices/the-dawn-of-the-ebomb>